eCH-0249 – Anforderungen an ein staatliches Identitäts-managementsystem (IdMS)

Name	Anforderungen an ein staatliches Identitätsmanagementsystem (IdMS)
eCH-Nummer	eCH-0249
Kategorie	Hilfsmittel
Reifegrad	Definiert
Version	1.0.0
Status	Genehmigt
Beschluss am	2022-09-07
Ausgabedatum	2022-12-08
Ersetzt Version	-
Voraussetzungen	-
Beilagen	-
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Fachgruppe-IAM Annett Laube, Gerhard Hassenstein
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Dieses Hilfsmittel beschreibt die wesentlichen Anforderungen von Benutzerinnen und Benutzern, sowie nutzenden Diensten an ein staatliches Identitätsmanagementsystem (IdMS). Dazu werden zuvor die möglichen Typen von Identitätsmanagementsystemen (IdMS) gegenübergestellt.

Inhaltsverzeichnis

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst die weibliche Form in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

1.1 Status

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

1.2 Anwendungsgebiet

Der erste Teil dieses Hilfsmittels beschreibt in Kapitel 1 und 2 die wesentlichen Unterschiede von Identitätsmanagementsystemen. Im zweiten Teil (ab Kapitel 3) wird auf die Anforderungen einer staatlichen elektronischen Identität eingegangen. Daraus ergeben sich die Aufgaben, die der Staat (auf Ebene Bund, Kanton oder auch Gemeinde) aus Sicht der nutzenden Dienste und Benutzer bieten sollte, um einen Vertrauensanker für eine staatliche Schweizer E-ID bilden zu können. In diesem Dokument wird davon ausgegangen, dass es sich bei der Schweizer E-ID um eine *E-Identity* entsprechend der Definition im IAM-Glossar (eCH-0219 [1]) handelt.

Die Anforderungen an ein staatliches IdMS werden technologieunabhängig beschrieben.

Die elektronische Identität eines Subjekts kann für viele Anwendungen mit sehr unterschiedlichen *Vertrauensstufen* (siehe eCH-0219 [1] bzw. eCH-0170 [2]) verwendet werden. Dieses Hilfsmittel beschränkt sich auf die *Authentifizierung* [1], welche an dieser Stelle für den Kontext der Schweizer E-ID genauer definiert wird:

Log-In (Authentifizierung):

Die elektronische Identität wird von seinem Inhaber zu *Log-in* Zwecken verwendet. Es geht darum, dass ein Subjekt gegenüber dem Online-Dienst beweisen muss, dass er wirklich der Inhaber der behaupteten elektronischen Identität ist. Diesen Beweis kann er unter Verwendung von verschiedenen Authentifizierungsfaktoren erbringen.

Eine erfolgreiche Authentifizierung ist Voraussetzung für weitere Aktionen, wie Autorisierung und Zugriff auf den Online-Dienst.

Mit dieser Definition lassen sich die häufigsten Anwendungsfälle abdecken:

- *Wiederkehrende Authentifizierung*: Die elektronische Identität wird vom Benutzer für das Login in eine dienstanbietende Organisation oder ein Ökosystem verwendet. → Verwendung innerhalb einer dienstanbietenden Organisation oder eines Ökosystems.
- *Einmaliges Onboarding*: Seine elektronische Identität (erstellt in einer anderen Organisation oder einem anderen Ökosystem) wird vom Benutzer für das Erstellen einer elektronischen Identität innerhalb einer dienstanbietenden Organisation oder eines Ökosystems verwendet. Die dienstanbietende Organisation oder das Ökosystem kann die elektronische Identität und Attribute des Benutzers verwenden. → Akzeptieren einer externen elektronischen Identität durch eine dienstanbietende Organisation oder ein Ökosystem.

Weitere Anwendungsbereiche, wie im Folgenden aufgeführt, sind prinzipiell ebenfalls möglich. Auf deren speziellere Anforderungen wird in diesem Hilfsmittel allerdings **nicht** eingegangen:

- **Digitale Signatur***:* Mit einer elektronischen Identität kann der Inhaber eine verbindliche Willensäusserung (qualifizierte Signatur) machen. Eine digitale Signatur beinhaltet nebst Herkunft (Authentizität) auch die Integrität der Daten. Eine digitale Signatur kann nur mit asymmetrischen Verfahren geleistet werden.
- **Speichern persönlicher Daten**: Der Benutzer bzw. Inhaber einer elektronischen Identität soll *persönliche Daten* abspeichern können und den Zugriff auf diese Dateien damit steuern können (z.B. mit SOLID[1]).
- **Offline-Nutzung:** Der Inhaber einer elektronischen Identität kann diese als Ersatz für seine physischen Ausweispapiere verwenden.
- …

1.3 Einordnung

Dieses Dokument verwendet generell Begriffe aus eCH-0219 – «IAM Glossar» [1], die mit den aufgeführten Begriffen aus Anhang C ergänzt werden. Es beruht auf den IAM Gestaltungsprinzipien [3] und kann unter den «Ergänzenden Hilfsmitteln» eingeordnet werden.

2 Vergleich Identitätsmanagementsysteme

Für die Einteilung von IdMS können aus **Benutzersicht** zwei Szenarien betrachtet werden: Zum einen ist dies die *Erstellung (bzw. Festlegung)* einer elektronischen Identität und zum anderen deren *Verwendung*. Dies führt zu den folgenden Fragen, welche als Kriterium für die Einteilung der IdMS verwendet werden können:

- Wer hat meine elektronische Identität ausgestellt und wer kennt sie?
- Wer ist bei der Verwendung dieser elektronischen Identität beteiligt?

Die IdMS werden nachfolgend anhand dieser Szenarien und Kriterien eingeteilt.

Szenario 1: Erstellung (bzw. Festlegung) einer elektronischen Identität

Für das erste Szenario, die Erstellung einer Identität, müssen folgende Fragen betrachtet werden:

- Wer führt meine Identitätsinformationen?
- An welche Stelle muss ich mich wenden, wenn ich eine Identität haben will?
- An welche Stelle muss ich mich wenden, wenn es zu meiner Identität eine Änderung gibt?

Dabei sind zwei Ausprägungen möglich:

[1] SOLID (SOcial LInked Data; https://solidproject.org/): hat die Dezentralisierung des gesamten World Wide Web als Ziel. Die Funktionsweise von Webanwendungen wird so geändert, dass der Benutzer effektiv die Hoheit über die eigenen Daten erhält, indem er die Plattform kontrolliert.

Prozess	Identitätsgebender Dienst	
		
Erstellung, Mutation, Löschung der elektronischen Identität	Identitätsdienst, dienstanbietende Organisation	Benutzer (Subjekt)

Tabelle 1 - Identitätsmaster

In einer ersten Variante wird die elektronische Identität eines Subjekts von einer externen Instanz vorgegeben oder der Benutzer erstellt seine Identität gemeinsam mit der externen Instanz. Auch wenn der Benutzer seine elektronische Identität selbst erstellt und sie dann erst übermittelt, gerät diese externe Instanz in Kenntnis der elektronischen Identität und der dazugehörigen Informationen. Eine solche externe Instanz kann eine dienstanbietende Organisation (z.B. Behörde oder Unternehmen) oder ein speziell dafür vorgesehener Dienst sein. Demgegenüber steht der benutzerzentrierte Ansatz. Hier erstellt der Benutzer seine elektronische Identität selbst, ohne dass diese einer anderen Instanz bekannt ist.

Szenario 2: Verwendung einer elektronischen Identität

Das zweite zu betrachtende Szenario für die Einteilung von IdMS ist die Verwendungsart. Auch hier gibt es zwei Möglichkeiten.

Prozess	Verbindung zum prüfenden Dienst	
		
Verwendung der Identität	Indirekte Verbindung	Direkte Verbindung

Tabelle 2 - Verwendungsart

Indirekte Verbindung: **Das Subjekt kann seine elektronische Identität nicht unabhängig von einer identitätsgebenden Instanz einsetzen**, denn diese Instanz muss die elektronische Identität des Subjekts zeitnah gegenüber der anfragenden Partei bestätigen, nachdem sich das Subjekt gegenüber dieser Instanz authentisiert hat.

Direkte Verbindung: Beim ***benutzerzentrierten*** Ansatz ist bei der Verwendung der elektronischen Identität kein Identitätsdienst involviert. ***Das Subjekt kann seine elektronische Identität unabhängig von einer identitätsgebenden Instanz einsetzen.*** Verwendung und Erstellung einer elektronischen Identität sind somit vollständig voneinander entkoppelt.

Diese beiden Szenarien (Erstellung und Verwendung[2]) können miteinander auf drei Arten kombiniert werden.

- Fremdbestimmung: Sowohl Erstellung wie auch die Verwendung der elektronischen Identität sind abhängig von einer identitätsgebenden Instanz.
- Teilkontrolle: Nur die Nutzung kann vom Benutzer kontrolliert werden, aber nicht die Erstellung.
- Vollständige Kontrolle: Ein Subjekt kann seine elektronische Identität selbst erstellen, ändern und nutzen.

In den folgenden Kapiteln werden diese Kombinationen näher beschrieben.

2.1 Fremdbestimmte Identität

Bei diesem klassischen Ansatz wird die elektronische Identität eines Subjekts von einer identitätsgebenden Instanz verwaltet.

Man unterscheidet zwei Instanzen, welche die elektronische Identität eines Subjekts erstellen können. Entweder die dienstanbietende Organisation selbst oder ein dafür spezialisierter Identitätsdienst.

2.1.1 Isolierte Identität

Wenn die elektronische Identität eines Subjekts (z.B. eines Kunden) von jeder dienstanbietenden Organisation einzeln vergeben und gepflegt wird, spricht man vielfach von **«isolierten»** Identitäten.

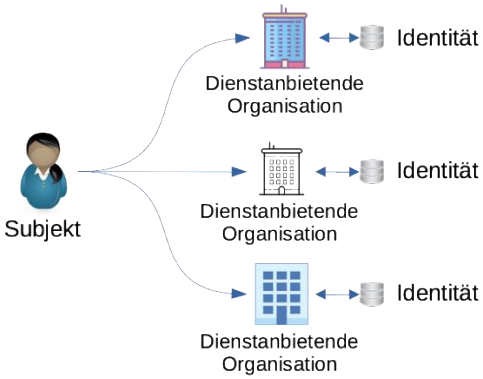

Abbildung 1: Eine elektronische Identität pro dienstanbietende Organisation (isoliert)

Folgende Eigenschaften können dieser verbreiteten Art zugewiesen werden:

- Die dienstanbietende Organisation unterhält eine Benutzerdatenbank (Kundendatenbank) mit den Anmeldedaten der von ihren kontrollierten Subjekten.
- Aus Sicht des Subjekts ist bis zu einem gewissen Grad der Schutz der Privatsphäre eingehalten, da pro dienstanbietende Organisation eine andere elektronische Identität vorliegen kann.

[2] Der Aspekt, wie ein Benutzer/Inhaber beweisen kann, dass er eine elektronische Identität unter seiner Kontrolle (oder in seinem Besitz) hat, bezieht sich auf die Bindung zwischen Subjekt und elektronischer Identität bzw. auf die Verwendung geeigneter Authentifizierungsmittel und wird in diesem Dokument nicht behandelt.

- Ein Subjekt muss pro dienstanbietende Organisation eine spezifische Identität pflegen (Identifikator und Authentifizierungsmittel), womit der Aufwand bei zunehmender Anzahl von Beziehungen steigt.
- Jede dienstanbietende Organisation definiert ihre eigenen Sicherheits- und Datenschutzrichtlinien[3], die alle unterschiedlich sein können (ein klassisches Beispiel sind die sehr unterschiedlichen Regeln für Passwörter).
- Die dienstanbietende Organisation ist dafür zuständig, Informationen ihrer Subjekte auf ihrer Seite sicher aufzubewahren. Wenn dies nicht erfolgreich getan werden kann, kann dies zu gravierenden Datenschutzverletzungen führen, wie einige Bespiele in der Vergangenheit gezeigt haben.
- Der Identifikator ist organisationspezifisch, deshalb sind auch die Identitätsdaten meist woanders nicht verwendbar. Beispiele dafür ist die Transportkunden-Identität aus dem ÖV oder die Switch edu-ID aus dem akademischen Bereich.

2.1.2 Spezieller Identitätsdienst

Eine dienstanbietende Organisation kann aber auch eine bereits bestehende elektronische Identität, welche im Vorfeld von einem speziellen Identitätsdienst erstellt wurde, mit dem Subjekt in ihrer Benutzerdatenbank verknüpfen.

Damit werden die Hauptnachteile (organisationsspezifische Identifikatoren und Aufbewahrung der Authentifizierungsmittel) einer isolierten Identität beseitigt. Die dienstanbietende Organisation übernimmt die Authentifizierung des Subjekts nicht mehr selbst, sondern delegiert diesen Prozessschritt an eine externe Instanz (Identitätsdienst), welcher sie vertraut (daher auch der Begriff der *«Relying Party»* bzw. *«vertrauende Partei»).* Das Subjekt muss sich für den Zugriff auf eine Ressource der dienstanbietenden Organisation erst beim **externen Identitätsdienst (IdP)** authentisieren und dieser meldet das Resultat der Anmeldung dann in geeigneter Form an den anfragenden Dienst der Organisation. Das Subjekt hat keine direkte Verbindung zur dienstanbietenden Organisation.

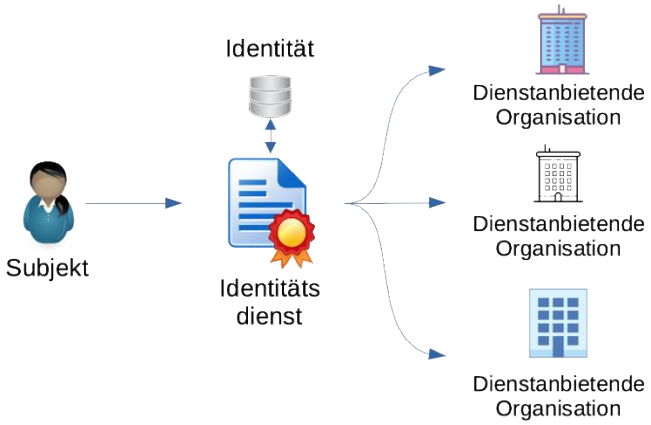

Abbildung 2: Eine elektronische Identität für mehrere dienstanbietende Organisationen (externer Identitätsdienst)

Dieser externe Identitätsdienst wird i.d.R. nicht nur eine Bestätigung der Authentifizierung übermitteln,

[3] Obschon übergeordnete Rahmenwerke in Form eines DSG [11] oder einer DSGVO existieren, werden Regeln oft unterschiedlich interpretiert. Die Internationalität von besuchten Diensten ist ein weiterer Faktor, welcher gemeinsame Datenschutzrichtlinien verunmöglichen.

sondern auch weitere Informationen zu diesem Subjekt (Attribute), für welche er im konkreten Fall zuständig ist. Die dienstanbietende Organisation erhält somit eine Kopie der Identitätsinformationen und legt diese zu den eigenen Daten in ihrer Benutzerverwaltung (Kundendatenbank) ab. Sie muss mit geeigneten Mitteln sicherstellen, dass die kopierten Daten aktualisiert werden, sofern dies für den Betreiber des Dienstes relevant ist.

In diesem Modell sind Identitätsdienst und dienstanbietende Organisation unterschiedliche organisatorische Einheiten, die miteinander kommunizieren müssen. Dienstanbietende Organisation und Identitätsdienst sind Teil einer Identitäts-Föderation. Die Kommunikation erfolgt über gängige Protokolle wie SAML [4], OAuth 2.0 [5] und OpenID Connect [6]. Diese Praxis hat sich mit dem Aufkommen sozialer Netzwerke wie Facebook, Google, Twitter, ... verstärkt. Facebook und Google z.B. stellen das typische Modell eines externen Identitätsdienstes dar. Aber auch andere Identitätsanbieter in der Cloud (z.B. Microsoft) sind hier erwähnenswert, da sie zunehmend von Unternehmen eingesetzt werden, um nebst Kunden auch ihre Mitarbeiter extern authentisieren zu lassen.

Für diese Art Identitätssystem können folgende Eigenschaften aufgeführt werden:

- Das Subjekt kann seine elektronische Identität und das damit verbundene Authentifizierungsmittel für alle Organisationen (Ökosysteme) verwenden, welche dem externen Identitätsdienst vertrauen.
- SSO über verschiedene Dienste der dienstanbietenden Organisationen ist einfach möglich.
- Die Auslagerung des ID-Managements an einen Identitätsdienst erlaubt es der dienstanbietenden Organisationen, Kosten und Aufwand zu sparen.
- Welche persönlichen Daten eines Subjekts erhoben werden, bestimmt meist der Identitätsdienst.
- Die persönlichen Daten, die eine dienstanbietende Organisation vom Identitätsdienst anfordert, ist für das Subjekt vielfach intransparent.
- Es gibt nicht einen Identitätsdienst für alle Webseiten und Anwendungen des täglichen Lebens. Daher braucht ein Subjekt immer noch mehrere Identitätsdienste.
- Identitätsdienste sind spezialisiert auf die Verwaltung von elektronischen Identitäten. Datensicherheit und Datenschutz der elektronischen Identitäten ist darum für sie eine existenzielle Notwendigkeit. Allerdings pflegt jeder Identitätsdienst seine eigenen Sicherheits- und Datenschutzrichtlinien, was eine Übersicht seitens Benutzer erschwert.
- Auch grosse Identitätsdienste können Opfer von Cyberkriminalität werden. Sie müssen grosse Infrastrukturen unterhalten und hohe Kosten auf sich nehmen, um eine sichere Speicherung zu gewährleisten, ähnlich wie beim isolierten Modell.
- Der externe Identitätsdienst wird in den Authentisierungsprozess zwischen Subjekt und Organisation eingebunden. Der Identitätsdienst weiss immer, wann und wo sich ein Subjekt angemeldet hat.
- Sowohl das Subjekt als auch die nutzende Organisation müssen einem Identitätsdienst vertrauen.[4] Das Subjekt muss darauf vertrauen können, dass der Identitätsdienst die Daten des

[4] Das Vertrauen zwischen Parteien wird einerseits durch die Definition von Pflichten/Rechte beider Partner und andererseits durch die Haftung, die bei einem durch Pflichtwidrigkeit verursachten Schaden zur Anwendung kommt, geregelt. Die Regelungen werden bei Behörden per Gesetz oder bei Privaten per Vertrag festgehalten.

Subjekts nicht missbraucht und die nutzende Organisation muss der Aussage eines Identitätsdiensts Glauben schenken.

- Da die Anzahl der Identitätsdienste relativ gering ist, ist eine Monopolisierung zu befürchten. Dies kann sich negativ auf die Transparenz auswirken.
- Benutzer fühlen sich oft unwohl, wenn ein Identitätsdienst all ihre Beziehungen und Anmeldeaktivitäten zu Organisationen verfolgen und überwachen kann.
- Konten auf einem Identitätsdienst sind nicht übertragbar. Wenn ein Identitätsdienst den Dienst einstellt, ist die elektronische Identität des Subjekts und sind damit verbundene Daten möglicherweise verloren.

2.2 Benutzerzentrierte Identität

Ein Identitätsmanagementsystem kann auch so aufgebaut werden, dass das Subjekt den Einsatz seiner Identitätsinformationen selbst kontrollieren kann. Dies hat den Vorteil, dass ein Identitätsdienst nicht mehr in den Anwendungsprozess (Authentisierung) zwischen Subjekt und Organisation eingebunden ist**. Die Ausstellung der elektronischen Identität ist von deren Verwendung entkoppelt** (auch zeitlich).

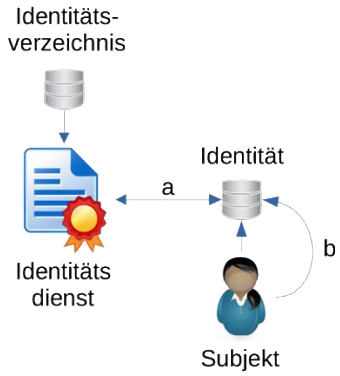

Abbildung 4: Erstellen einer elektronischen Identität

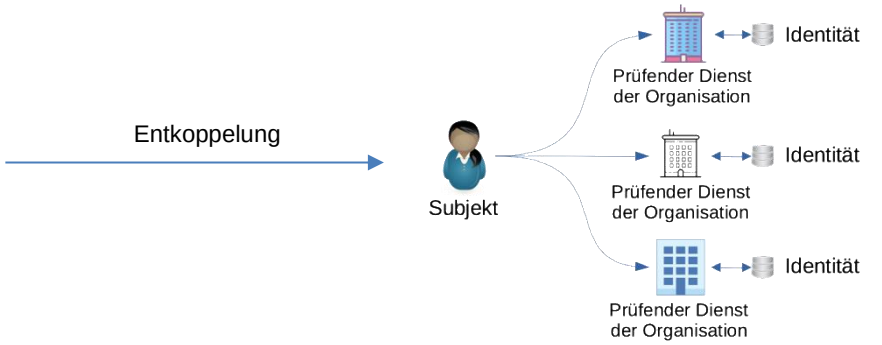

Abbildung 3: Verwenden der elektronischen Identität

Die elektronische Identität wird von einem Identitätsdienst für ein Subjekt erstellt (a). Diese wird dem Subjekt in einer bestimmten Form (z.B. als X.509-Zertifikat oder Verifiable Credential) zur Aufbewahrung übergeben (Kapitel 2.2.1). Das Subjekt erhält somit nur die Kontrolle über die Verwendung seiner elektronischen Identität (Teilkontrolle). Das Subjekt hat eine direkte Verbindung zum prüfenden Dienst der Organisation. Das Subjekt kann aber auch selbst seine elektronische Identität erstellen (b). In diesem Fall übernimmt das Subjekt die Kontrolle bei der Erstellung und bei der Verwendung seiner Identität (Kapitel 2.2.2).

Neben den grossen Vorteilen, die die zeitliche Entkopplung bei der Nutzung einer benutzerzentrierten elektronischen Identität und die Kontrolle durch das Subjekt bieten, sind unter anderem folgende Punkte zu beachten:

- *Agenten (agents - delegation):* Wenn ein Subjekt seine elektronische Identität einem speziell dafür vorgesehenen Dienst (Agent) anvertraut und diesem alle notwendigen Privilegien erteilt, so ist das Prinzip der alleinigen Kontrolle über die eigene elektronische Identität nicht mehr gegeben. Das Subjekt muss diesem Agenten somit voll vertrauen.

- *Interoperabilität (interoperability):* Das Prinzip der Interoperabilität [7] besagt, dass ein Benutzer jederzeit seine elektronische Identität und die damit verbundenen Attribute (Verifiable Credentials) auf interoperable Weise unter Verwendung offener, öffentlicher und gebührenfreier Standards verwenden, austauschen und sichern kann. Diese Anforderung ist heute nur schwerlich erreichbar.
- *Portabilität (portability):* Wie kann ein Benutzer seine elektronische Identität auf mehreren Devices (Desktop, Notebook, Handy, Tablet) speichern und verwenden? Dieser Anspruch ist sehr legitim. Dazu muss ein Benutzer ein Backup haben, um dieses auf dem anderen System wiederherstellen zu können. Alternativ können auch Geräte direkt eine vertrauenswürdige Synchronisation der Daten anstossen.
- *Vertrauen (trust):* Ein verifizierender Dienst muss zu den vom Subjekt präsentierten Informationen ein Vertrauen aufbauen können. Man unterscheidet zwischen «technischem Vertrauen» (z.B. Überprüfung einer Signatur) und einem «sozialen Vertrauen» in den Aussteller, welches von einer Community (Gemeinschaft) erarbeitet und an ihre Mitglieder weitergeben wird.

Eine umfassende Erklärung zu elektronischen Identitäten und IdMS ist unter [8] zu finden.

2.2.1 Teilkontrollierte Identität

Die elektronische Identität eines Subjekts wird im Vorfeld von einem Identitätsdienst unabhängig (oder unter Mitwirkung des Subjekts) erstellt und dem **Subjekt zur Kontrolle und Aufbewahrung übergeben**. Der Vorteil ist, dass der Identitätsdienst nur noch beim Ausstellen (und bei der Aktualisierung) aktiv ist. Der Nachteil ist aber, dass das Subjekt wenig Einfluss auf den Erstellungs- und Übergabeprozess hat. Das Subjekt muss also ein genügend grosses Vertrauen in diesen Identitätsdienst haben.
Beim Zugriff auf eine dienstanbietende Organisation präsentiert das Subjekt seine Identitätsinformationen in verlangter Form (z.B. als X.509-Zertifikat oder QR-Code). Der prüfende Dienst der Organisation kann nach der Präsentation die Herkunft und Gültigkeit der Identitätsinformationen prüfen. Je nach Ausgestaltung dieser Identitätsinformationen, können diese auch in der physischen Welt verwendet werden.

Bei Verlust der elektronischen Identität kann sich das Subjekt an den Identitätsdienst wenden, um diese ersetzen zu lassen, oder ggf. in einem ersten Schritt zu revozieren.

Typisches Beispiel eines selbstkontrollierten IdMS ist der nPA (neuer Personalausweis der Bundesrepublik Deutschland) [9].

2.2.2 Vollständig kontrollierte Identität

Dieser Ansatz kommt gänzlich **ohne zentralen Identitätsdienst** aus und ist als «Self-Issued Identity» oder «Self-sovereign Identity» (SSI) bekannt. In dieser Variante **erstellt und verwendet** das Subjekt seine elektronische Identität selbst. Diese elektronische Identität kann optional in einem dezentralen Identitätsverzeichnis verlinkt werden. Das Subjekt kann sich in der Folge Attribute (einzeln oder als Gruppe) von autoritativen Quellen (Aussteller) bestätigen lassen. Dazu muss sich das Subjekt bei einem Aussteller zunächst authentisieren und seine selbstdeklarierten Eigenschaften bestätigen lassen (Aussage). Das Subjekt «sammelt» so bestätigte Attribute (z.B. *Verifiable Credentials*) zu seiner elektronischen Identität, welche es dann aufbereitet und bei Bedarf einem prüfenden Dienst (Verifier)

in verlangter Form präsentiert, z.B. als *Verifiable Presentation*.

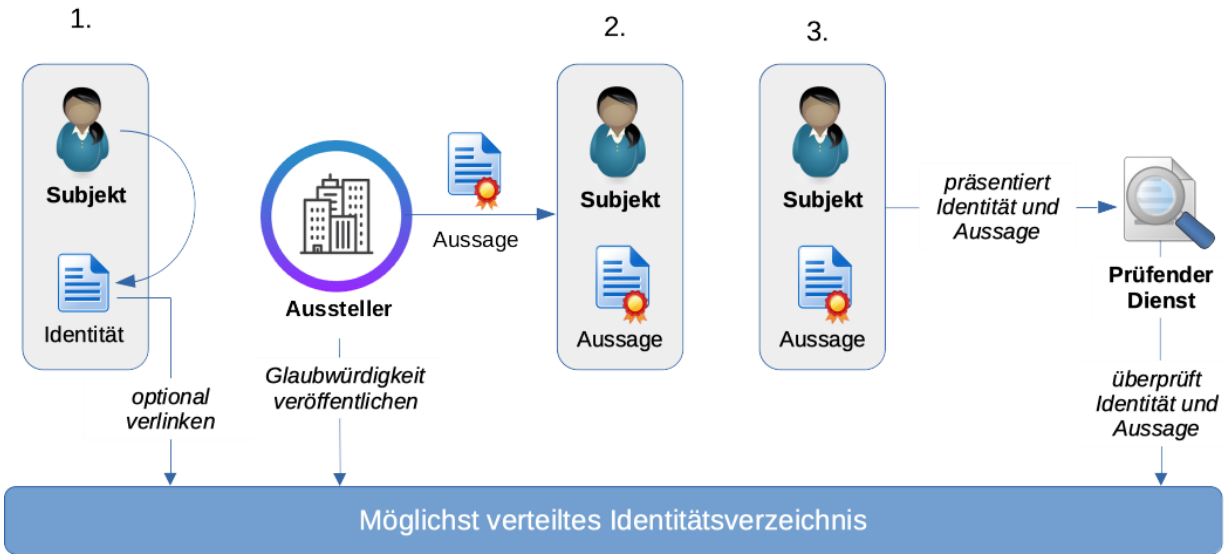

Abbildung 5: Selbstverwaltete Identität

Der prüfende Dienst muss sich in irgendeiner Form, von der ihm präsentierten elektronischen Identität und den zugehörigen Aussagen überzeugen können. Dazu wurden verschiedene Ansätze implementiert. Diese reichen von der Übermittlung von Verifiable Credentials [10] in ihrer ursprünglichen Form bis hin zu Zero Knowledge Proofs (ZKP). Dem Subjekt wird bei dieser Variante grösstmögliche Autonomie, aber auch ein grosses Mass an Verantwortung übertragen.

Eine «selbstverwaltete Identität» erfordert viel mehr Verantwortung des Benutzers, da es keine Instanz gibt, die ihm bei Problemen unterstützen kann. Dazu zählen u.a.:

- *Wiederherstellung (recovery):* Ein Subjekt muss seine selbsterstellte Identität sowie die gesammelten Aussagen in einer vertrauenswürdigen und sicheren Umgebung ablegen können. → Digitale Brieftasche (Wallet). Um das Prinzip der alleinigen Kontrolle über seine elektronische Identität bei einer Hinterlegung (Backup) nicht zu verlieren, müssen persönliche Daten so abgelegt werden, dass nur das Subjekt selbst (oder Subjekte mit entsprechender Berechtigung) darauf zugreifen können. Verschiedene Lösungsvarianten wurden in diesem Zusammenhang bereits vorgeschlagen und umgesetzt (Guardian-Systeme, Social Key-Recovery, etc.).

2.3 Vergleich von IdMS-Typen

Wenn die verschiedenen IdMS Typen anhand der in Kapitel 2 definierten Szenarien und Kriterien untersucht und gegenübergestellt werden, ergibt sich folgendes Bild:

	Fremdbestimmt	Benutzerzentriert	
		Teilkontrolliert	vollständig kontrolliert
Aussteller der elektronischen Identität	Identitätsdienst	Identitätsdienst	Subjekt
Kontrolle über die **elektronische** Identität	Identitätsdienst	Subjekt	Subjekt
Kontrolle über das Authentisierungsmittel	Subjekt	Subjekt	Subjekt
Bestätigung der Basisidentität	Identitätsdienst	Identitätsdienst	Identität ist zuerst selbstdeklariert und wird später von einer autoritativen Quelle bestätigt.
Bestätigung von Attributen	Identitätsdienst bzw. andere autoritative Quellen	Identitätsdienst bzw. andere autoritative Quellen	Attribute sind zuerst selbstdeklariert und werden später von einer autoritativen Quelle bestätigt.
Authentifizierung	Identitätsdienst	Prüfender Dienst der Organisation	Prüfender Dienst der Organisation
Wiederherstellung der Identitätsinformationen bei Verlust	Identitätsdienst	Identitätsdienst	Subjekt ist selbst verantwortlich → Sichere Schlüsselhinterlegung oder Delegation an einen Dritten.

Tabelle 3 – Vergleich der IdMS-Typen aus Sicht des Benutzers

3 Anforderungen an ein staatliches IdMS

Der Staat und politische Entscheidungsträger müssen sich auf die Bereitstellung nationaler elektronische Identitäten und ID-Dokumente sowie die Schaffung eines technisch-rechtlichen Rahmens (Basisinfrastruktur) einstellen.

In der Folge werden diese Anforderungen an eine Basisinfrastruktur zusammengestellt.

- Der Staat soll eine nationale, von Privaten und Behörden nutzbare **Infrastruktur** bereitstellen.

Damit können sich Transaktionsparteien darauf abstützen. Es ist gerade bei der Einführung neuer Technologien sehr wichtig, eine nationale Standardisierung vorzugeben.

- Transaktionsparteien (Personen und Organisationen) sollen die Vereinbarungen, Verfahren und die Nachrichtenübermittlungen bilateral steuern können.
- Nutzende Parteien müssen sich auf die Herkunft und Unveränderheit (Integrität) von Identitätsdaten verlassen können → **technische Überprüfbarkeit**.
- Die nutzende Partei muss sich auf die rechtliche Verbindlichkeit vom Inhaber getätigter Aussagen verlassen können. Auch darauf, dass die Aussage tatsächlich vom berechtigten Inhaber stammt.
- Der Staat soll nicht eigene Protokoll-Standards definieren, sondern Lösungen auf bestehende Protokolle (idealerweise basierend auf internationalen Standards) etablieren. Eine vom Staat vorgegebene Identitätslösung muss auf einem **offenen Konzept** beruhen, welches jederzeit an neue technologische Entwicklungen angepasst werden kann.
- Die Infrastruktur sollte kompatibel mit E-ID-Lösungen aus dem europäischen Umfeld sein, wenn dies ohne Abschwächung der Vertrauensstufen und der Verbindlichkeit möglich ist.

Für Identitätsdaten eines Subjektes sollte der Staat folgende Grundsätze beachten:

- Ein Benutzer kann sich gegenüber einer autoritativen Quelle **nicht anonym** verhalten. Bevor ein Herausgeber (z.B. ein Heimatstaat) eine beglaubigte Aussage in irgendeiner Form ausstellt, muss er den Benutzer identifizieren. Nur so können sich konsumierende Dienste auf Identitätsinformationen verlassen → Der Staat ist demnach in der Rolle einer autoritativen Quelle aller Informationen zu einer Basisidentität, welche er garantieren kann.
- Dies gilt auch für andere autoritative Quellen, denn sie steuern Informationen zumeist basierend auf der Basisidentität des Staates bei.[5]
- Diese Basisidentität kann der Staat als x.509-Zertifikat und/oder als Verifiable Credentials ausstellen. Wichtig dabei ist, dass die ausgestellten Identitätsinformationen eines Benutzers von dessen Applikation und vom Endempfänger (nutzenden Dienst) interpretiert werden können.

3.1 Anforderungen der Bürger[6]

Auf der einen Seite soll der Staat seinen Bürgern ermöglichen, sicher und einfach[7] an der digitalen Welt teilzuhaben. Ein Bürger, als Benutzer einer staatlichen E_ID, hat auf der anderen Seite bestimmte Anforderungen gegenüber einem prüfenden Dienst, um den Missbrauch seiner Daten zu verhindern.

Nebst Benutzerfreundlichkeit, Interoperabilität und Portabilität muss eine Lösung unter anderem folgende Merkmale aufweisen:

[5] Wenn eine autoritative Quelle einem Subjekt Bestätigungen ohne Bezug zur Basisidentität, d.h. auf der Basis einer anderen elektronischen Identität ausstellt, erschwert das die gemeinsame Verwendung dieser Bestätigungen u.U. erheblich (Multi-credential verification).

[6] Der Begriff «Bürger» wird in diesem Dokument stellvertretend für alle Einwohner und Einwohnerin der Schweiz verwendet.

[7] Benutzerfreundlichkeit und -zufriedenheit sind ausschlaggebend für eine breite Nutzung. Die Nutzung der E-ID sollte bequem, transparent und dennoch verständlich sein.

- **Selektive Offenlegung** (selective disclosure): Der Benutzer muss die Möglichkeit haben, jederzeit einer prüfenden Instanz nur diejenigen persönlichen Informationen (inkl. Identifikatoren) preiszugeben, welche er will.
- **Datensparsamkeit** (data economy): Ein prüfender Dienst darf nur die minimal notwendigen Attribute eines Benutzers verlangen, welche für eine Geschäftsbeziehung notwendig sind (geregelt in [11]).
- **Anonymität** (anonymity): In den meisten Fällen kann sich ein Benutzer gegenüber einem prüfenden Dienst nicht anonym verhalten. Im Normalfall will dieser die elektronische Identität des Benutzers kennen, wenn er die Attribute überprüft. Aber die eingesetzte Technologie muss die Anonymität des Benutzers voll unterstützen. Der Benutzer muss die Möglichkeit haben, seine elektronische Identität gegenüber einem prüfenden Dienst vollständig verdecken zu können. Diese Anforderung ist nur dann möglich, wenn eine prüfende Partei sich von bestimmten Informationen eines Benutzers überzeugen kann, ohne diese konkret zu kennen. Die Einhaltung der Anonymität eines Benutzers ist demnach nur mit speziell dafür vorgesehenen Verfahren (z.B. wie abgeleitete Attribute oder Zero Knowledge Proofs) möglich.
- **Nicht-Verknüpfbarkeit** (unlinkability): Der Benutzer muss bei der Verwendung seiner Identitätsinformationen davon ausgehen können, dass kein eindeutiger Identifikator (einschliesslich des öffentlichen Schlüssels) an mehrere prüfende Dienste[8] übertragen wird, welcher es diesen ermöglicht, die elektronische Identität des Benutzers auf einfache Art und Weise vervollständigen zu können (Profilbildung) oder diese an Dritte weiterzugeben.
- **Revokation:** Der Benutzer muss in der Lage sein, seine Identität jederzeit zu deaktivieren und Attribute revozieren zu lassen.

Weiterhin stellen sich zwei Fragen, die ein Benutzer selbst nicht beantworten kann:

- Ist ein Dienst berechtigt, als E-ID nutzender Dienst aufzutreten? Beispielsweise ist die Versicherung «xyz» berechtigt, als solche im Netz ihre Dienste anzubieten? Bisher wurde das Webserver Zertifikat [12] - welches von einer berechtigten Instanz ausgestellt wurde - vom Browser validiert. Aber auf Berechtigung wurde bislang nicht geprüft.
- Welche Identitätsinformationen (z.B. Name, Geschlecht, AHV-Nummer, RP-übergreifender eindeutiger Identifikator[9], ...) dürfen von diesem Dienst erhoben werden, damit eine Geschäftsbeziehung mit dem Benutzer[10] aufgebaut werden kann?

Die Berechtigungen des E-ID nutzenden Dienstes sollte der Staat regulieren. Er sollte bestimmen, auf welche Informationen des Subjekts ein E-ID nutzender Dienst in welchem Fall/unter welchen Umständen zugreifen darf und ob ein nutzender Dienst die Berechtigung hat, in dieser Rolle aufzutreten. Der Staat muss die Umsetzung aber nicht selbst machen, sondern kann die Überwachung und Vergabe

[8] Das kann durch individuelle Identifikatoren pro nutzenden Dienst erreicht werden.

[9] Eindeutige Identifikatoren sind besonders kritisch, da dadurch eine Zusammenführung der Aktivitäten des Benutzers bei verschiedenen nutzenden Diensten (Profilbildung) möglich wird, die auch zur Überwachung missbraucht werden kann (siehe auch: https://epicenter.works/content/orwells-wallet-das-elektronische-identifizierungssystem-der-eu-fuehrt-uns-direkt-in-den).

[10] Nicht zu verwechseln mit der Zustimmung des Benutzers (user consent), in welcher er bestimmt, welche seiner Identitätsinformationen mit dem nutzenden Dienst geteilt werden sollen.

an eine Trägerschaft delegieren, welche die nutzenden Dienste besser kennt (z.B. an ein Ökosystem).

3.2 Anforderungen der nutzenden Dienste

Ein Paradigmenwechsel auf benutzerzentrierte Identitätssysteme und die Etablierung neuer Technologien (sofern dies angestrebt wird) muss vom Staat, vom Benutzer wie auch von den nutzenden Diensten unterstützt werden.

Für einen nutzenden Dienst ergeben sich in seiner Funktion die folgenden Hauptanforderungen:

- **Prüfung & Berechtigung:** Der nutzende Dienst muss zeitnah überprüfen[11] können, ob die ihm präsentierten Attribute echt und unverändert sind und für diesen Benutzer ausgestellt wurden. Er muss von einem nutzenden Dienst auch überprüft werden können, ob ein Herausgeber berechtigt ist, eine Aussage über den Benutzer zu machen.
- Ein nutzender Dienst muss zusätzlich folgende Kriterien überprüfen können:
  - Entsprechen die präsentierten Identitätsinformationen den verlangten Attributen?
  - Sind die präsentierten Identitätsinformationen interpretierbar?
  - Kann eine Zugriffskontrolle mit den präsentierten Identitätsinformationen gemacht werden?
- **Nichtabstreitbarkeit:** Beim Onboarding erhält der nutzende Dienst einen Identifikator, der einen eindeutigen Rückschluss auf den Benutzer ermöglicht und somit die Nichtabstreitbarkeit gem. den regulatorischen Vorgaben, z.B. GWG-Gesetz [13], innerhalb der geltenden Aufbewahrungsfristen garantiert.

3.3 Zusammenspiel «Staat – Bürger – Nutzende Organisation»

	Staat	Bürger	Nutzende Organisation
Basisinfrastruktur	Bestimmt, erstellt und unterhält eine Basisinfrastruktur.	Der Benutzer verwendet die bestehende Basisinfrastruktur.	Der nutzende Dienst verwendet die bestehende Basisinfrastruktur.
Berechtigung	Betreibt eine Registry, in welcher die Trägerschaften / Organisationen pro Ökosystem hinterlegt werden.	Die Applikation des Benutzers überprüft die Berechtigung des online Dienstes	Die Organisation lässt sich von einer Trägerschaft / Staat berechtigen, dass sie in einem bestimmten Ökosystem auftreten kann.
Elektronische Identität	Der Staat erstellt die elektronische Identität des Benutzers und übergibt sie diesem (benutzerzentriert).	Der Benutzer kontrolliert die Nutzung seiner elektronischen Identität.	Die Organisation prüft die staatliche elektronische Identität und kann diese mit der ihren verbinden.

[11] Eine zeitnahe Überprüfung schliesst eine Prüfung auf Revokation der Identität bzw. einzelner Attribute ein.

	Staat	Bürger	Nutzende Organisation
Standards	Der Staat als Identitätsanbieter einigt sich zusammen mit den nutzenden Organisationen auf Standards.	Der Benutzer profitiert von Portabilität und Interoperabilität durch die genutzten Standards.	Akzeptiert die zusammen mit den Identitätsanbietern erarbeiteten Standards.

Tabelle 4 – Zusammenspiel Staat - Bürger - Nutzende Organisation

4 Fazit

Der Staat soll die notwendige Basisinfrastruktur vorgeben. Diese beinhaltet aber nicht unbedingt einen allgemein verwendbaren nationalen Identitätsdienst, d.h. der nationale Identitätsdienst wird nur zur Ausstellung der EID verwendet, aber nicht für die (wiederkehrende) Authentifizierung und für das Onboarding bei nutzenden Diensten.

Mit «fremdverwalteten» Systemen können heutzutage nicht mehr alle Anforderungen an ein staatliches IdMS abdeckt werden. Insbesondere der Anspruch an einen erhöhten Schutz der Privatsphäre steht einem «fremdverwalteten» System im Weg. Eine «fremdverwaltete» Identitätslösung macht nur dann Sinn, wenn der Schutz der Privatsphäre eines Subjekts keine grosse Rolle spielt oder ein Vertrauen in einen Identitätsdienst vorausgesetzt werden kann. Beides ist nur im Rahmen einer Organisation (oder eines Ökosystems) gegeben, ähnlich einem «Trusted-Third-Party» System.

Im «freien» Internet eignet sich eine «fremdverwaltete» Identitätslösung schlecht, wenn Vertrauen und Schutz der Privatsphäre verlangt wird. Es gäbe zu viele Sicherheitsrichtlinien, die zwischen dem Identitätsdienst und dem Online-Dienst vereinbart werden müssten, da sie grundsätzlich unterschiedlichen Organisationen angehören. Soziale Medien verwenden zwar dieses Konstrukt, aber sie verfolgen damit ganz andere Ziele (business cases). Der Staat sollte sich mit der Herausgabe einer «seriösen» teilkontrollierten elektronischen Identität von sozialen Medien abgrenzen.

5 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

6 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

[1] eCH, «eCH-0219 IAM Glossar, Version 1.0,» 30 November 2018. [Online]. Available: http://ech.ch/de/standards/39940.

[2] eCH, «eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten, V2.0,» 13 September 2017. [Online]. Available: https://ech.ch/index.php/de/standards/60593.

[3] eCH, «eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM), Version 3.0,» 07 Februar 2019. [Online]. Available: https://ech.ch/de/standards/60198.

[4] OASIS, «Security Assertion Markup Language (SAML) V2.0 Technical Overview,» 25 March 2008. [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[5] Internet Engineering Task Force (IETF) , «The OAuth 2.0 Authorization Framework,» 01 October 2012. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6749.

[6] J. B. M. J. B. d. M. a. C. M. N. Sakimura, «OpenID Connect Core 1.0 incorporating errata set 1,» 8 November 2014. [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html.

[7] Sovrin Foundation , «Die Grundsätze von SSI,» 16 Dezember 2020. [Online]. Available: https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-German-v01.pdf.

[8] T. Ruff, «The Three Models of Digital Identity Relationships,» 24 April 2018. [Online]. Available: https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186.

[9] Bundesministerium des Innern, für Bau und Heimat, «Der Personalausweis mit Online-Ausweisfunktion,» 2020. [Online]. Available: https://www.bmi.bund.de/DE/themen/moderne-verwaltung/ausweise-und-paesse/personalausweis/personalausweis-node.html.

[10] W3C, «Verifiable Credentials Data Model v1.1,» 09 Novmbeer 2021. [Online]. Available: https://www.w3.org/TR/vc-data-model/.

[11] «Bundesgesetz über den Datenschutz (DSG),» 1 März 2019. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de.

[12] CA/Browser Forum, «EV SSL Certificate Guidelines,» [Online]. Available: https://cabforum.org/extended-validation/.

[13] «Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG),» 1 Januar 2022. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/de.

Anhang B – Mitarbeit & Überprüfung

<Hier sind alle Mitarbeiterinnen und Mitarbeiter aufzuführen, die an dieser Version des Dokuments mitgearbeitet haben.>

Dominic Baumann	BFH
Michael Doujak	Ergon AG
Michael Gerber	
Gerhard Hassenstein	BFH
Christian Heimann	Fedpol
Annett Laube	BFH
Esther Hefti	Kanton ZH

Anhang C – Abkürzungen und Glossar

In diesem Kapitel werden zusätzliche oder abgewandelte Begriffe zum aus eCH-0219 – «IAM Glossar» [1] aufgeführt, die in eine neue Version des eCH-0219 übernommen werden sollten.

Abkürzungen

EID	Elektronische Identität (engl. Electronic Identity)
IdMS	Identitätsmanagementsystem
IdP	Identitätsdienst (engl. Identity Provider)
nPA	Neuer Personalausweis
SSI	«Self-Issued Identity» oder «Self-sovereign Identity»
SSO	Single Sign-on (SSO)
ZKP	Zero Knowledge Proof

Glossar

- **Anonymität:** Anonymität ist das Gegenteil eines Nachweises der Identität. Beides schliesst sich gegenseitig aus.
- **Aussteller (engl. Issuer)**
  Ein Aussteller beglaubigt Eigenschaften eines Subjekts als Attribute in einem standardisierten Format (z.B. SAML-Assertion, JWS, Verifiable Credential). Ein IdP kann als Aussteller agieren.
- **Basisidentität**: Die Basisidentität ist eine staatlich regulierte elektronische Identität, welche aus einem eindeutigen Identifikator und Personeninformation, wie Name, Geburtsdatum und

Gesichtsbild, besteht.

- **Identitätsmanagement-System (IdMS)**
  Synonym für *IAM-System*
- **Inhaber (engl. Holder):** Der Benutzer (Subjekt), für den die Berechtigungsnachweise ausgestellt werden und der diese bei sich, z.B. in seiner digitalen Brieftasche, aufbewahrt.
- **Dienstanbietende Organisation**
  Eine Organisation, die einen oder mehrere fachliche Online-Dienste (RPs) ihren Benutzern (Subjekten) anbietet.
- **Identitätsdienst**
  Eine Identitätsdienst verwaltet und stellt Identitäten aus. Ein Identitätsdienst kann einen online Authentifizierungsdienst und Attributbestätigungsdienst enthalten.
- **Identitätsverzeichnis**
  In einem zumeist dezentralem Identitätsverzeichnis können optional elektronische Identitäten und deren Attribute (Verifiable Credentials) zum Zwecke der Überprüfung (Verifikation) von Existenz und Vertrauenswürdigkeit, verlinkt werden. Auch Informationen zu Deaktivierung/Revokation können hier abgelegt werden.
- **Ökosystem**
  Ein Ökosystem ist eine Gruppe von dienstanbietenden Organisationen, die dieselben Benutzer-Identitäten verwenden, z.B. ÖV oder Gesundheitswesen.

Anhang D – Änderungen gegenüber Vorversion

Dies ist die erste Version.

Anhang E – Abbildungsverzeichnis

Anhang F – Tabellenverzeichnis